UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,650	12/20/2001	Anton C. Rothwell	NAI1P056/01.187.01	2721

28875 7590 06/30/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
CHEA, PHILIP J	
ART UNIT	**PAPER NUMBER**
2153	

DATE MAILED: 06/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/028,650	ROTHWELL ET AL.	
	Examiner	Art Unit	
	Philip J. Chea	2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This Action is in response to an Amendment filed March 30, 2005. Claims 1-29 are currently pending. Any rejection not set forth below has been overcome by the current Amendment.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-32,34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al. (US 5,968,176), and further in view of Reid et al. (US 6,182,226) in view of Vaidya (US 6,279,113).

As per claim 1, Nessett et al. disclose a network adapter system, as claimed, comprising:

- a processor positioned on a network adapter coupled between a computer and a network (see column 11, lines 26-31, where network adapter is considered the NIC; computer is considered the end system, and the processor is inherent within the NIC for it to operate);
- wherein the processor is adapted for content scanning of network traffic transmitted between the computer and the network (see column 11, lines 54-62, where scanning is implied by filtering within a NIC to implement a multilayer firewall).

Although the system disclosed by Nessett et al. shows substantial features of the claimed invention (discussed above), it fails to disclose virus scanning to scan for known types of malicious programs or data.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Nessett et al., as evidenced by Reid et al.

In an analogous art, Reid et al. disclose a system where a firewall maintains a set of regions restricting communication according to a set of policies (see Abstract). Further, teaching the firewall

containing a virus scanner region to scan for known type of malicious program or data (see Fig. 4, and column 8, lines 10-18).

Given the teaching of Reid et al., a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Nessett et al. by employing a firewall capable of virus scanning to scan for known types of malicious programs or data, such as disclosed by Reid et al., in order to further improve the level of security provided by a firewall to prevent malicious attacks from incurring on a target system.

Although the system disclosed by Nessett et al. in view of Reid et al. shows substantial features of the claimed invention (discussed above), it fails to disclose that the virus scanning utilizes virus signature files.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Nessett et al. in view of Reid et al., as evidenced by Vaidya.

In an analogous art, Vaidya discloses an intrusion detection system where there are attack signature profiles to aid in monitoring network traffic. Further showing the intrusions being unauthorized manipulation of network data and attempted delivery of malicious data packets (see column 3, lines 12-26),

Given the teaching of Vaidya, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Nessett et al. in view of Reid et al. by scanning for virus signature files, such as disclosed by Vaidya, in order to accurately monitor for viruses, and distinguish between different types of attacks to address them accordingly.

As per claim 2, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the processor is capable of being user-configured (see Nessett et al. column 16, lines 31-42).

As per claim 3, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the processor is capable of being user-configured locally (see Nessett et al. column 20, lines 62-67, where it is implied if there is a storage available at the node, the configuration data will be available to the node locally; and nodes are devices as described by Nessett et al. in column 8, 1-6)

As per claim 4, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the processor is capable of being user-configured remotely via a network connection with the network adapter (see Nessett et al. column 16, lines 31-42).

As per claim 5, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the processor is capable of being user-configured only after the verification of a password (see Nessett et al. column 18, lines 11-19).

As per claim 6, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the manner in which the scanning is performed is capable of being user-configured (see Nessett et al. column 17, lines 9-21).

As per claim 7, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the settings of the network adapter are capable of being user-configured (see Nessett et al. column 20, lines 42-46, where the settings are considered the rules that are being configured in the node).

As per claim 8, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the processor is capable of determining whether received packets are of interest (see Nessett et al. column 23, lines 18-26).

As per claim 9, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the packets of interest are based on an associated protocol (see Nessett et al. column 23, lines 18-26, where the associated protocol is considered protocols other than FTP in this case).

As per claim 10, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the processor is capable of passing received packets that are not of interest to the computer (see Nessett et al. column 23, lines 18-26).

As per claim 11, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the processor is capable of scanning received packets that are of interest (see Nessett et al. column 23, lines 18-26, where scanning is implied from the ability to distinguish between the different protocols).

As per claim 12, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the processor is capable of denying received packets that fail the scan (see Nessett et al. column 23, lines 18-26).

As per claim 13, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the scan is performed based on user settings (see Nessett et al. column 23, lines 43-57, where the user settings are determined by the user configured Multilayer Firewall Management Station).

As per claim 30, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the content scanning enforces operational policies of an organization (see Nessett et al. column 17, lines 9-21).

As per claim 31, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the policies include detecting entities selected from the group consisting of harassing content, pornographic content, junk e-mails, and misinformation (see Vaidya column 3, lines 12-26).

As per claim 32, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that it would have been obvious to store the signature files on a non-volatile solid state memory on the network adapter since virus scanning is performed on the network adapter, it would be obvious that the signature files be located along with the virus scanner.

As per claim 34, Nessett et al. in view of Reid et al. in view of Vaidya further disclose that the packets that are of interest include executable files (see Vaidya et al. column 11, lines 35-47).

As per claim 14,27,28 Nessett et al. disclose a system for scanning network traffic on a network adapter, as claimed, comprising:

- network adapter means for receiving packets (see column 23, lines 18-26);
- processor means positioned on the network adapter means for content scanning of the packets (see column 23, lines 18-26); and
- means for conditionally taking security measures if the packets fail the scan (see column 23, lines 18-26).

Although the system disclosed by Nessett et al. shows substantial features of the claimed invention (discussed above), it fails to disclose virus scanning to scan for known types of malicious programs or data.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Nessett et al., as evidenced by Reid et al.

In an analogous art, Reid et al. disclose a system where a firewall maintains a set of regions restricting communication according to a set of policies (see Abstract). Further, teaching the firewall containing a virus scanner region to scan for known type of malicious program or data (see Fig. 4, and column 8, lines 10-18).

Given the teaching of Reid et al., a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Nessett et al. by employing a firewall capable of virus scanning to scan for known types of malicious programs or data, such as disclosed by Reid et al., in order to further improve the level of security provided by a firewall to prevent malicious attacks from incurring on a target system.

Although the system disclosed by Nessett et al. in view of Reid et al. shows substantial features of the claimed invention (discussed above), it fails to disclose that the virus scanning utilizes virus signature files.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Nessett et al. in view of Reid et al., as evidenced by Vaidya.

In an analogous art, Vaidya discloses an intrusion detection system where there are attack signature profiles to aid in monitoring network traffic. Further showing the intrusions being unauthorized manipulation of network data and attempted delivery of malicious data packets (see column 3, lines 12-26),

Given the teaching of Vaidya, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Nessett et al. in view of Reid et al. by scanning for virus signature files, such as disclosed by Vaidya, in order to accurately monitor for viruses, and distinguish between different types of attacks to address them accordingly.

As per claims 15-26, see rejection for claims 2-13 above.

As per claim 29, Nessett et al. disclose a network adapter system, as claimed, comprising:

- a processor positioned on a network adapter coupled between a computer and a network, the processor including a packet assembly module, random access memory, and a scanner module (see column 23, lines 18-26, where processor components claimed are inherent within the processor disclosed by Nessett et al.).
- a user interface driver for identifying network traffic of interest transmitted between the computer and the network (see column 23, lines 18-26);
- wherein the processor is adapted for discerning and content scanning of network traffic of interest transmitted between the computer and the network (see column 23, lines 18-26).

Although the system disclosed by Nessett et al. shows substantial features of the claimed invention (discussed above), it fails to disclose virus scanning to scan for known types of malicious programs or data.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Nessett et al., as evidenced by Reid et al.

In an analogous art, Reid et al. disclose a system where a firewall maintains a set of regions restricting communication according to a set of policies (see Abstract). Further, teaching the firewall containing a virus scanner region to scan for known type of malicious program or data (see Fig. 4, and column 8, lines 10-18).

Given the teaching of Reid et al., a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Nessett et al. by employing a firewall capable of virus scanning to scan for known types of malicious programs or data, such as disclosed by Reid et al., in order to further improve the level of security provided by a firewall to prevent malicious attacks from incurring on a target system.

Although the system disclosed by Nessett et al. in view of Reid et al. shows substantial features of the claimed invention (discussed above), it fails to disclose that the virus scanning utilizes virus signature files.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Nessett et al. in view of Reid et al., as evidenced by Vaidya.

In an analogous art, Vaidya discloses an intrusion detection system where there are attack signature profiles to aid in monitoring network traffic. Further showing the intrusions being unauthorized manipulation of network data and attempted delivery of malicious data packets (see column 3, lines 12-26),

Given the teaching of Vaidya, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Nessett et al. in view of Reid et al. by scanning for virus signature files, such as disclosed by Vaidya, in order to accurately monitor for viruses, and distinguish between different types of attacks to address them accordingly.

3. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al. in view of Reid et al. in view of Vaidya as applied to claim 32 above, and further in view of Bonomo et al. (US 6,658,562).

Although the system disclosed by Nessett et al. in view of Reid et al. in view of Vaidya shows substantial features of the claimed invention (discussed above), it fails to disclose that memory is user protected by configuring a network adapter BIOS with a password that only a user can change.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Nessett et al. in view of Reid et al. in view of Vaidya, as evidenced by Bonomo.

In an analogous art, Bonomo discloses a system for setting different BIOS configurations stored in a memory device (see Abstract). Further showing setting a password to view information in a BIOS setup program or to change configuration (see column 4, lines 11-21 and 30-41).

Given the teaching of Bonomo, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Nessett et al. in view of Reid et al. in view of Vaidya by employing a password protected BIOS, such as disclosed by Bonomo, in order to prevent unwanted users from changing settings without authorization.

Response to Arguments

4. Applicant's arguments filed March 30, 2005 have been fully considered but they are not persuasive.

(A) Applicant contends that Nessett's disclosure of a firewall does not teach scanning for network traffic.

In considering (A), the Examiner respectfully disagrees. In order to filter packets such as disclosed by Nessett. The firewall must implicitly scan packets to determine if they are blocked or allowed through. To filter packet traffic each packet must be looked at, which is interpreted as being scanned.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Philip J. Chea whose telephone number is 571-272-3951. The examiner can normally be reached on M-F 7:00-4:30 (1st Friday Off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenn Burgess can be reached on 571-272-3949. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Philip J Chea
Examiner
Art Unit 2153

PJC 6/20/05

Bradley Edelman
Art Unit 2153